

KDDI Business ID
SAML認証対応サービス SSO設定マニュアル
別紙

Salesforce SSO設定マニュアル

Version 1.0

Tomorrow. Together



- 本マニュアルでは、KDDI Business IDにおけるSalesforceとのSSO設定手順をご案内します。
- 本マニュアルは「[KDDI Business ID SAML認証対応サービス SSO設定マニュアル](#)」の別紙の位置付けとなりますので、併せてご確認ください。
- 設定を開始するために、次の前提条件を満たしている必要があります。
 - Salesforceをご利用中で、管理者アカウントにてログインできる状態であること。
 - Salesforceを「カスタムドメイン」にて利用している、もしくは利用予定であること。
 - SSO利用予定のユーザについて、My KDDI Biz (旧KDDI ビジネスオンラインサポート) のユーザIDとSalesforceのID[メールアドレス]が一致していること。
- Salesforce側の仕様変更等により設定方法が変わる場合があります。
- Salesforce側の仕様／動作／不具合に関するご質問につきましては、KDDI Business IDのサポート対象外とさせていただきますので予めご了承ください。

[Step1] KDDI Business ID メタデータダウンロード

- ① My KDDI Biz (旧KDDI ビジネスオンラインサポート) に管理者アカウントでログイン
- ② サービス → SSO設定をクリック
- ③ 追加をクリック → SSOサービス追加 (入力) 画面へ遷移



④ IdPメタデータをクリックしファイル「metadata.xml」を保存(後の手順で使用)

⑤ 証明書ををクリック

⑥ ダウンロードをクリックしてファイル「certificate.crt」を保存(後の手順で使用)

⑦ この画面はそのままとした状態で、別画面で次手順へ進む

[Step2] Salesforce SSO設定 (1)



① Salesforceに管理者アカウントでログイン

② クイック検索ボックスに「シングルサインオン設定」と入力し、
[シングルサインオン設定] を選択

③ 編集をクリック

シングルサインオン設定

[このページのヘルプ](#)

外部の環境から Salesforce のユーザーを認証するには、シングルサインオンを設定します。組織で使用できるシングルサインオンのオプションは次のとおりです。

- 代理認証は、Salesforce からエンドポイントに送られる Web サービスコールを使用するシングルサインオンメソッドです。
- 統合認証は、Salesforce のエンドポイントに送られる SAML アサーションを使用するシングルサインオンメソッドです。

[編集](#) [SAML アサーション検証](#)

代理認証

Salesforce ログイン情報を使用したログインを無効化

SAML を使用した統合シングルサインオン

SAML を有効化

統合 ID の大文字と小文字を区別しないように設定

SAML シングルサインオン構成

[新規](#) [メタデータファイルから新規作成](#) [メタデータ URL から新規作成](#)

アクション	名前	SAML のバージョン	発行者	エンティティ ID
編集 削除	...	2.0
編集 削除	...	2.0

[Step2] Salesforce SSO設定 (2)

シングルサインオン設定

<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	
代理認証	
Salesforce ログイン情報を使用したログインを無効化 <input type="checkbox"/>	
SAML を使用した統合シングルサインオン	
SAML を有効化 <input checked="" type="checkbox"/>	統合 ID の大文字と小文字を区別しないように設定 <input type="checkbox"/>
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

④ SAML を有効化にチェック

⑤ [保存] をクリック

[Step2] Salesforce SSO設定 (3)

シングルサインオン設定

外部の環境から Salesforce のユーザを認証するには、シングルサインオンを設定します。組織で使用できるシングルサインオンのオプションは次のとおりです。

- 代理認証は、Salesforce からエンドポイントに送られる Web サービスコールを使用するシングルサインオンメソッドです。
- 統合認証は、Salesforce のエンドポイントに送られる SAML プラッシュを使用するシングルサインオンメソッドです。

編集 SAML アサーション検証

代理認証
Salesforce ログイン情報を使用したログインを無効化

SAML を使用した統合シングルサインオン
SAML を有効化 統合 ID の大文字と小文字を区別しないように設定

SAML シングルサインオン構成

アクション	名前	SAML のバージョン	発行者	エンティティ ID
編集 削除	11111111	2.0	<<<<<<<	https://example.com
編集 削除	22222222	2.0	<<<<<<<	https://example.com
編集 削除	33333333	2.0	<<<<<<<	https://example.com

⑥ SAML シングルサインオン設定で、メタデータファイルから新規作成をクリック

⑦ メタデータファイルの「ファイルを選択」から Step1の④でダウンロードした「metadata.xml」を指定

⑧ 作成をクリック

SAML シングルサインオン構成

ID プロバイダの SAML 2.0 設定を含む XML ファイル (1 MB 以下) を使用して、設定を作成します (Salesforce はこのファイルを保存しません)。

作成 キャンセル

メタデータファイル 選択されていません

作成 キャンセル

[Step2] Salesforce SSO設定 (4)

SAML シングルサインオン構成

このページのヘルプ

名前

SAML のバージョン 2.0

API 参照名

発行者

エンティティ ID

ID プロバイダの証明書 選択されていません

現在の証明書
有効期限: 2023-01-01 00:00:00 ~ 2023-01-01 00:00:00

証明書の署名要求

署名要求メソッド

アサーション番号化証明書

SAML ID 種別 アサーションには、ユーザの Salesforce ユーザ名が含まれます
 アサーションには、ユーザオブジェクトの統合 ID が含まれます
 アサーションには、ユーザオブジェクトのユーザ ID が含まれます

SAML ID の場所 ID は、Subject ステートメントの NameIdentifier 要素にあります
 ID は Attribute 要素にあります

サービスプロバイダの起動要求バインド HTTP ポスト
 HTTP リダイレクト

警告: メタデータファイルは、ログイン URL に対して複数のバインドを指定します。

ID プロバイダのログイン URL

ID プロバイダのログアウト URL

カスタムログアウト URL

カスタムエラー URL

シングルログアウトを有効にする

ジャストインタイムのユーザプロビジョニング 必須情報

ユーザプロビジョニングの有効化

保存 保存 & 新規 キャンセル

⑨名前にKDDI Business IDと入力

⑩ID プロバイダの証明書の「ファイルを選択」から Step1の⑥でダウンロードした「certificate.crt」を指定

⑪サービスプロバイダの起動要求バインドで「HTTP ポスト」を選択

⑫カスタムログアウト URLに「https://businessportal.kddi.com/」を指定

⑬保存をクリック

[Step2] Salesforce SSO設定 (1)

①左側メニューよりドメイン管理> 私のドメインをクリック

②認証設定の編集をクリック

The image shows a screenshot of the Salesforce mobile app interface. On the left is a navigation menu with a search bar at the top. The menu items include 'ホーム' (Home), '管理' (Admin), and '私のドメイン' (My Domain), which is highlighted with a red box. An arrow points from this menu item to the main content area on the right. The main content area is titled '私のドメインの設定' (My Domain Settings) and contains several sections: '私のドメインの詳細' (My Domain Details), 'ルーティング' (Routing), 'ポリシー' (Policies), and '認証設定' (Authentication Settings). The '認証設定' section has a red box around its '編集' (Edit) button. The '認証設定' section also includes a note: 'この組織のすべてのリリース済みおよびプロビジョニング済みドメインに認証構成設定が適用されます。' (Authentication configuration is applied to all released and provisioned domains in this organization.)

[Step2] Salesforce SSO設定 (5)

③認証サービスの項目でStep2の⑨で入力した名前(KDDI Business ID)にチェックを入れる

④保存をクリック

認証設定

認証設定

ログインページ種別 ▼

認証サービス

- ログインサービス
- KDDI Business ID
- KDDI Business ID (旧)
- KDDI Business ID (旧)
- KDDI Business ID (旧)
- KDDI Business ID (旧)
- KDDI Business ID (旧)

ロゴファイル 選択されていません

背景色

右フレームの URL

iOS でのユーザ認証にネイティブブラウザを使用

Android でのユーザ認証にネイティブブラウザを使用

- ① Step1のMy KDDI Biz (旧KDDI ビジネスオンラインサポート) の画面に戻る
- ② サービス → SSO設定をクリック
- ③ 追加をクリック → SSOサービス追加 (入力) 画面へ遷移

The screenshot shows the 'SSOサービス追加 (入力)' form. At the top, there is a navigation bar with 'ユーザ', 'サービス+', 'セキュリティ+', 'ログ', and '契約情報'. Below the navigation bar, the form title is 'SSOサービス追加 (入力)'. The form contains several sections: '追加SSOサービス' with a dropdown menu set to 'Salesforce'; 'サービス名 (必須)' with a text input field containing 'Salesforce'; 'アイコン (必須)' with a 'Salesforce' icon and an 'アップロード' button; 'メタデータ' with an 'アップロード' button; 'ACS URL (必須)' with a text input field containing a long alphanumeric string; 'Entity ID (必須)' with a text input field containing a long alphanumeric string; 'Name ID フォーマット' with a dropdown menu set to 'UNSPECIFIED'; 'Name ID ソース' with a dropdown menu set to 'ユーザID'; and '属性情報' with a table for '属性名' and '属性値'. At the bottom, there are 'キャンセル' and '確認' buttons.

④ サービス「Salesforce」を選択

⑤ メタデータにStep1の⑥でダウンロードした「SAMLSP-XXXX.xml」を指定してアップロード

※以下の入力項目は変更せず初期値のままにしてください。
(Name IDフォーマット: 「UNSPECIFIED」、
Name IDソース: 「ユーザID」、属性情報: なし)
※サービス名とアイコンは任意のものに変更可能です。
(設定したアイコンとサービス名がユーザのホーム画面に表示されます。)

⑧ 確認をクリック → SSOサービス追加 (確認) 画面へ遷移

⑨ 内容を確認し完了をクリック → SSOサービス一覧画面へ遷移

- ① Salesforce側のSSO利用ユーザが未登録の場合、Salesforceにてユーザを登録
- ② My KDDI Biz (旧KDDI ビジネスオンラインサポート) にてユーザを登録
(その際、SalesforceのユーザIDと同じIDとすること)
- ③ My KDDI Biz (旧KDDI ビジネスオンラインサポート) にてユーザへSalesforceをサービス追加登録

※②③の手順については、[マニュアル本編](#)の第2章を参照してください。

これ以降、ユーザによるSSOが可能となります。